UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,697	01/20/2004	Yuji Suga	CFA00044US	3352

7590 02/12/2007

Canon U.S.A. Inc.
Intellectual Property Department
15975 Alton Parkway
Irvine, CA 92618-3731

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/761,697	Applicant(s) SUGA, YUJI	
	Examiner Martin Jeriko P. San Juan	Art Unit 2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-23 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-23 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 9/9/05.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This is a response to the following case application:
Non-provisional Application No 10/761697 filed on January 20, 2004.

Specification

1. The information disclosure statement filed "1-out-of-n Proof with Decreased Proof Length" fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

2. The information disclosure statement filed "1-out-of-n Proofs – Ring Signatures based on the DLP" fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

3. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, applications, or other information submitted for consideration by the Office, and MPEP § 609.04(a), subsection I. states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Paragraph [0021] – C.P. Schnorr, "Efficient Signature Generation by Smart Cards."

4. The disclosure is objected to because of the following informalities:

Spelling error: "manger" change to "manager" [Par 0028, Ln 3]

Appropriate correction is required.

Claim Objections

1. Claim 3, 7, and 12 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim.

Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

2. Claim 13 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim on (11 or 12) and 1. See MPEP § 608.01(n). Accordingly, this claim and claim 14 have not been further treated on the merits.

3. Claim 17 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim on 1 and 11. See MPEP § 608.01(n). Accordingly, this claim has not been further treated on the merits.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Independent claims 1, 2, 11, 18, 19, 20, and dependent claims 3-10, 12-17, and 21-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Although claims 1-13, and 14-16 preambles recite "apparatus," there are no recitations to either a machine or a manufacture. Rather, the limitations are directly to software per se, which are not a statutory category of invention.

Although claim 17 preamble recites a system, the limitations teach apparatus with no recitations to either a machine or a manufacture, but rather directly to software per se, which are not a statutory category of invention.

Furthermore, claims 21-23 are software per se, which are not a statutory category of invention, because they lack the structure necessary to make the claim a machine.

Independent claims 1, 2, 11, 18-20, and dependent claims 3-10, 12-17, and 21-23 are directed to a judicial exception (specifically an abstract idea). The independent claims lack a practical application of the judicial exception because there are no tangible results.

Claim 1 recites denial data generating means.
Claim 2 recites hash computing means, pseudo computing means, and signing means.
Claim 11 recites hash computing means, verification computational-operation means, and verifying means.
Claim 18 recites a denial data generating step.

Claim 19 recites a hash computing step, pseudo computing step, and a signing step.
Claim 20 recites a hash computing step, verification computational-operation step, and a verifying step.

While all these claims recite limitations having resultant data, there is no evidence or clear evidence that all data are readily made available for use.

The corresponding dependent claims also lack a practical application of the judicial exception because there are no tangible results as described above. Furthermore, these dependent claims fail to correct the lack of a practical application of their parent claims:

Claim 3 recites an apparatus having an alternative means of operation in a digital signature system.
Claim 4 recites a means for creating denial data.
Claim 5 recites pledge-data attaching means, accompanying-data extracting means, re-signing means, and denial-data outputting means.
Claim 6 recites hash re-computing means, and computational-operation means.
Claim 7 recites a replacement of pledge data with pre-computed data.
Claim 8 recites a resultant pre-computed data.
Clam 9 recites an apparatus having an alternative means of security protocol.
Claim 10 recites denial data proven by interactive communication.
Claim 12 recites a message changed to the executed digital signature system.
Claim 13 recites means for generating denial data.
Claim 14 recites signature-massage receiving means, ring-signature data receiving means, denial-data receiving means, pledge-data receiving means, accompanying-data extracting means, hash computational-operation means, denial data verifying means.
Claim 15 recites an apparatus having an alternative means of security protocol.
Claim 16 recites denial data proven by interactive communication.
Claim 17 recites the ring signature apparatus and the ring signature verifying apparatus.
Claim 21-23 are software per se.

Claim Rejections - 35 USC § 112

1. Claims 3, 7, 9-10, 12 and 15-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 9 and 15, “security based on discrete logarithm problem” is vague and indefinite because it is unclear how this kind of security is related to the parent claims.

Regarding claims 10 and 16, "proven by interactive communication" is vague and indefinite because it is unclear from the parent claims on how denial data is to be proven by this limitation.

Regarding claims 3, 7, and 12, these claims are vague and indefinite because it is unclear how these limitations claimed serve to further limit the parent claim. Furthermore it is impermissible to broaden the scope of dependent claim relative to the parent claim.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

a. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

A. Claims 1-4, 8-12, 15, 16, and 18-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oishi (US PN: 6154841) (hereinafter Oishi) as applied to all claim above, and further in view of Rivest et al (NPL #1), and Abe et al (NPL #3).

(1) On the basis of independent claim 1, Oishi teaches a Group Signature Creating apparatus comprising of:

(a) Signature data inputting [starting at Col 16, Ln 27] means for inputting Group signature data that can be created with N public keys and a private key corresponding to one of the N public keys, that allows for signature verification for each of the N public keys, and

(b) Denial-data generating [starting at Col 17, Ln 56] means for generating denial data in accordance with the Group signature data, the denial data allowing for verification that a user other than a creator of the Group signature data has not signed.

(2) On the basis of independent claim 2, Oishi teaches a Group Signature creating apparatus comprising of:

(a) Hash computing means for generating first pre-computed data [starting Col. 14, Ln 35] and computing an j-th hash value for data [Col. 16, Ln. 65] that has N public keys [Col 14, Ln 45] and at least one private key corresponding to the N public keys [Col 14, Ln 46] and that includes the message [Col. 16, Ln 56] and a j-th pre-computed data [Col 16, Ln 64];
(b) Pseudo computing means for computing the j-th pre-computed data [Col 16, Ln 38 and 40], and an j-th signature data such that the j-th hash value appears to have been signed [Col 17, Ln 2-4] (Note that pre-computed data as defined in the context of the Specification is interpreted as any needed data that must be available at the start of a cryptographic algorithm whether that would be a hash function or the generation of the signature itself); and
(c) Signing means for generating first signature data corresponding to the first pre-computed data from the private key, with respect to an N-th hash value obtained through sequential computing by the pseudo computing means [Col 17, Ln 2-4].

(3) Based from the noted objection/rejection, dependent claim 3 will be interpreted to recite the same limitations as that of its parent claim 2. Hence dependent claim 3 is rejected based on the same rationale as that of its parent claim 2.

(4) With regard to dependent claim 4, the applicant recites the same limitation as that of Claim 1, pertaining specifically to the denial-data generating means. Dependent claim 4 is rejected based on the same analysis and rationale as that of its parent claim 2 and the same analysis and rationale as that of independent claim 1 pertaining specifically to the limitation on the denial-data generating means.

(5) With regard to dependent claim 8, Oishi teaches a Group Signature creating apparatus wherein the first pre-computed data is a result of computation in which with respect to a generator g of a multiplicative group of order P-1, pseudo random number k is generated and a computational operation g^k (mod P) is performed, where P is a prime number and k < P-1 [Col 8, Ln 60-67, thru Col 9, Ln 1-26]. This limitation is inherent to the Schnorr signature cryptography as implemented and shown by Oishi in his Group Signature scheme.

(6) With regard to dependent claim 9, Oishi teaches a Group Signature creating apparatus wherein security is based on a discrete logarithm problem [Col 17, Ln 60].

(7) With regard to dependent claim 10, Oishi teaches a Group Signature creating apparatus wherein the denial data is proven by interactive communication using Zero Knowledge Proof protocol [Col 18, Ln 1-36].

(8) On the basis of independent claim 11, Oishi teaches a Group Signature verifying apparatus comprising:

(a) hash computing means for computing an i-th hash value for data [Col. 16, Ln. 65] that has N public keys [Col. 14, Ln. 45] and that includes the message [Col. 16, Ln 56] and an i-th pre-computed data [Col 16, Ln 64];
(b) verification computational-operation means for performing a computational operation for verification of an i-th signature data [Col 18, Ln 4];
(c) and verifying means for verifying whether an N-th bit commitment value, BC, matches the verifier's BC value, the BC values being obtained through sequential computation by the verification computational-operation means [Col 18, Ln 4].

Oishi does not teach "hash values" per se. It would have been obvious to one of ordinary skill in the art at the time of the invention to implement a different verification protocol thereby modifying the bit commitment values to the "hash values" presented by the applicant while keeping the same architecture as that of Oishi's.

(9) Based from the noted objection/rejection, dependent claim 12 will be interpreted to recite the same limitations as that of its

parent claim 11. Hence dependent claim 12 is rejected based on the same analysis and rationale as that of its parent claim 11.

(10) With regard to dependent claim 15, Oishi teaches a Group Signature verifying apparatus wherein security is based on a discrete logarithm problem [Col 17, Ln 60].

(11) With regard to dependent claim 16, Oishi teaches a Group Signature verifying apparatus wherein the denial data is proven by interactive communication using Zero Knowledge Proof protocol [Col 18, Ln 1-36].

(12) Independent claim 18 is rejected using the same analysis and rationale of claim 1, because claim 18 has the same limitations as claim 1, and is merely the method of using the apparatus of claim 1.

(13) Independent claim 19 is rejected using the same analysis and rationale of claim 2, because claim 19 has the same limitations as claim 2, and is merely the method of using the apparatus of claim 2.

(14) Independent claim 20 is rejected using the same analysis and rationale of claim 11, because claim 20 has the same limitations as claim 11, and is merely the method of using the apparatus of claim 11.

(15) Dependent claim 21 is rejected using the same analysis and rationale of its parent claim 18, because claim 21 has the same limitations of its parent claim 18, and is merely the subroutines that will be identical to the methods of claim 18.

(16) Dependent claim 22 is rejected using the same analysis and rationale of its parent claim 19, because claim 22 has the same limitations of its parent claim 19, and is merely the subroutines that will be identical to the methods of claim 19.

(17) Dependent claim 23 is rejected using the same analysis and rationale of its parent claim 20, because claim 23 has the same limitations of its parent claim 20, and is merely the subroutines that will be identical to the methods of claim 20.

With regard to claims 1-4, 8-12, 15, 16, and 18-23, Oishi does not teach a Ring signature scheme. A Ring Signature is a "simplified group signature scheme that have only users and no managers." (Rivest et al, 2001), therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the Group Signature cryptographic methods or scheme to that of a Ring signature type as taught by Abe et al (disclosed by the applicant in the Specifications as prior art) because Ring signatures provide the improvement of manager/administrator exclusion.

B. Claims 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oishi (US PN: 6154841) (hereinafter Oishi) as applied to all claim above, and further in view of Rivest et al (NPL #1), Abe et al (NPL #3) and Canard et al (US 2006/0155985 A1).

(1) With regard to dependent claim 5, Oishi teaches a Group Signature creating apparatus according to claim 4, further comprising: message receiving means for receiving a message attached to a signature [Col 12, Ln 12]; Group signature data receiving means for receiving the Group signature data in which a signature data is attached to the message [Col 17, Ln 5]; parameter data attaching means for attaching parameter data to the message to be sent as Group signature [Col 15, Ln 23]; signature-data parameter extracting means for extracting data parameters as this is inherent because it is needed to compute a signature parameter data from the received Group signature data for verification [Col 17, Ln 5]; signing means for generating a signature comprising the parameter data attached message created by the parameter-data attaching means [Col 17, ln 2]; and signature-data outputting means for outputting Group signature computed by the signing means [Col 17, Ln 2].

Oishi does not teach pledge-data per se, but it would have been obvious to one of ordinary skill in the art at the time of the invention to modify signature data parameters to generate a new parameter data, in this case pledge-data, to forge a new group signature that can indicate denial or a form of revoking anonymity. Re-signing to prove ownership has been exploited as a form of revoking anonymity [Canard et al., US 2006/0155985 A1, Page 6, par 0131]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the contrapositive of re-signing to prove ownership, which in this case is the forging a new signature to indicate non-ownership, based from the original message and original public key corresponding to a unique private/secret key.

(2) With regard to dependent claim 6, Oishi teaches a Group Signature creating apparatus according to claim 5, wherein the signing means comprises hash computing means for computing a hash value for data obtained from a signature/certificate [Col 16, Ln 51] and computational-operation means for performing a computational operation on the hash value computed by the hash computing means [Col 17, Ln 1].

(3) Based from the noted objection/rejection, dependent claim 7 will be interpreted to recite the same limitations as that of its parent claim 5. Hence dependent claim 7 is rejected based on the same rationale as that of its parent claim 5.

With regard to claims 5-7, Oishi does not teach a Ring signature scheme. A Ring Signature is a "simplified group signature scheme that have only users and no managers." (Rivest et al, 2001), therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the Group Signature cryptographic methods or scheme to that of a Ring signature type as taught by Abe et al (disclosed by the applicant in the Specifications as prior art) because Ring signatures provide the improvement of manager/administrator exclusion.

C. Claims 1-4, 8-12, 15, 16, and 18-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oishi (US PN: 6154841) as applied to all claim above, and further in view of Naor et al (NPL #2), and Abe et al (NPL #3).

(1) On the basis of independent claim 1, Oishi teaches a Group Signature Creating apparatus comprising of:

(a) Signature data inputting [starting at Col 16, Ln 27] means for inputting Group signature data that can be created with N public keys and a private key corresponding to one of the N public keys, that allows for signature verification for each of the N public keys, and
(b) Denial-data generating [starting at Col 17, Ln 56] means for generating denial data in accordance with the Group signature data, the denial data allowing for verification that a user other than a creator of the Group signature data has not signed.

(2) On the basis of independent claim 2, Oishi teaches a Group Signature creating apparatus comprising of:

(d) Hash computing means for generating first pre-computed data [starting Col. 14, Ln 35] and computing an j-th hash value for data [Col. 16, Ln. 65] that has N public keys [Col 14, Ln 45] and at least one private key corresponding to the N public keys [Col 14, Ln 46] and that includes the message [Col. 16, Ln 56] and a j-th pre-computed data [Col 16, Ln 64];
(e) Pseudo computing means for computing the j-th pre-computed data [Col 16, Ln 38 and 40], and an j-th signature data such that the j-th hash value appears to have been signed [Col 17, Ln 2-4] (Note that pre-computed data as defined in the context of the Specification is interpreted as any needed data that must be available at the start of a cryptographic algorithm whether that would be a hash function or the generation of the signature itself); and
(f) Signing means for generating first signature data corresponding to the first pre-computed data from the private key, with respect to an N-th hash value obtained through sequential computing by the pseudo computing means [Col 17, Ln 2-4].

(3) Based from the noted objection/rejection, dependent claim 3 will be interpreted to recite the same limitations as that of its parent claim 2. Hence dependent claim 3 is rejected based on the same rationale as that of its parent claim 2.

(4) With regard to dependent claim 4, the applicant recites the same limitation as that of Claim 1, pertaining specifically to the denial-data generating means. Dependent claim 4 is rejected based on the same analysis and rationale as that of its parent claim 2 and the same analysis and rationale as that of independent claim 1 pertaining specifically to the limitation on the denial-data generating means.

(5) With regard to dependent claim 8, Oishi teaches a Group Signature creating apparatus wherein the first pre-computed data is a result of computation in which with respect to a generator g of a multiplicative group of order P-1, pseudo random number k is generated and a computational operation g^k (mod P) is performed, where P is a prime number and k < P-1 [Col 8, Ln 60-67, thru Col 9, Ln 1-26]. This limitation is inherent to the Schnorr signature cryptography as implemented and shown by Oishi in his Group Signature scheme.

(6) With regard to dependent claim 9, Oishi teaches a Group Signature creating apparatus wherein security is based on a discrete logarithm problem [Col 17, Ln 60].

(7) With regard to dependent claim 10, Oishi teaches a Group Signature creating apparatus wherein the denial data is proven by interactive communication using Zero Knowledge Proof protocol [Col 18, Ln 1-36].

(8) On the basis of independent claim 11, Oishi teaches a Group Signature verifying apparatus comprising:

(d) hash computing means for computing an i-th hash value for data [Col. 16, Ln. 65] that has N public keys [Col. 14, Ln. 45] and that includes the message [Col. 16, Ln 56] and an i-th pre-computed data [Col 16, Ln 64];
(e) verification computational-operation means for performing a computational operation for verification of an i-th signature data [Col 18, Ln 4];
(f) and verifying means for verifying whether an N-th bit commitment value, BC, matches the verifier's BC value, the BC values being obtained through sequential computation by the verification computational-operation means [Col 18, Ln 4].

Oishi does not teach "hash values" per se. It would have been obvious to one of ordinary skill in the art at the time of the invention to implement a different verification protocol thereby modifying the bit commitment values to the "hash values" presented by the applicant while keeping the same architecture as that of Oishi's.

(9) Based from the noted objection/rejection, dependent claim 12 will be interpreted to recite the same limitations as that of its parent claim 11. Hence dependent claim 12 is rejected based on the same analysis and rationale as that of its parent claim 11.

(10) With regard to dependent claim 15, Oishi teaches a Group Signature verifying apparatus wherein security is based on a discrete logarithm problem [Col 17, Ln 60].

(11) With regard to dependent claim 16, Oishi teaches a Group Signature verifying apparatus wherein the denial data is proven by

interactive communication using Zero Knowledge Proof protocol [Col 18, Ln 1-36].

(12) Independent claim 18 is rejected using the same analysis and rationale of claim 1, because claim 18 has the same limitations as claim 1, and is merely the method of using the apparatus of claim 1.

(13) Independent claim 19 is rejected using the same analysis and rationale of claim 2, because claim 19 has the same limitations as claim 2, and is merely the method of using the apparatus of claim 2.

(14) Independent claim 20 is rejected using the same analysis and rationale of claim 11, because claim 20 has the same limitations as claim 11, and is merely the method of using the apparatus of claim 11.

(15) Dependent claim 21 is rejected using the same analysis and rationale of its parent claim 18, because claim 21 has the same limitations of its parent claim 18, and is merely the subroutines that will be identical to the methods of claim 18.

(16) Dependent claim 22 is rejected using the same analysis and rationale of its parent claim 19, because claim 22 has the same limitations of its parent claim 19, and is merely the subroutines that will be identical to the methods of claim 19.

(17) Dependent claim 23 is rejected using the same analysis and rationale of its parent claim 20, because claim 23 has the same limitations of its parent claim 20, and is merely the subroutines that will be identical to the methods of claim 20.

With regard to claims 1-4, 8-12, 15, 16, and 18-23, Oishi does not teach a Ring signature scheme. Since the Ring Signature is a "generalization of the Group Signature" (Naor, 2002), it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the Group Signature cryptographic methods or scheme to that of a Ring signature type as taught by Abe et al (disclosed by the applicant in the Specifications as prior art) because Ring signatures provide the improvement of manager/administrator exclusion.

Claims 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oishi (US PN: 6154841) (hereinafter Oishi) as applied to all claim above, and further in view of Naor (NPL #2), Abe et al (NPL #3) and Canard et al (US 2006/0155985 A1).

(4) With regard to dependent claim 5, Oishi teaches a Group Signature creating apparatus according to claim 4, further comprising: message receiving means for receiving a message attached to a signature [Col 12, Ln 12]; Group signature data receiving means for receiving the Group signature data in which a signature data is attached to the message [Col 17, Ln 5]; parameter data attaching means for attaching parameter data to the message to be sent as Group signature [Col 15, Ln 23]; signature-data parameter extracting means for extracting data parameters as this is inherent because it is needed to compute a signature parameter data from the received Group signature data for verification [Col 17, Ln 5]; signing means for generating a signature comprising the parameter data attached message created by the parameter-data attaching means [Col 17, ln 2]; and signature-data outputting means for outputting Group signature computed by the signing means [Col 17, Ln 2].

Oishi does not teach pledge-data per se, but it would have been obvious to one of ordinary skill in the art at the time of the invention to modify signature data parameters to generate a new parameter data, in this case pledge-data, to forge a new group signature that can indicate denial or a form of revoking anonymity. Re-signing to prove ownership has been exploited as a form of revoking anonymity [Canard et al., US 2006/0155985 A1, Page 6, par 0131]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the contrapositive of re-signing to prove ownership, which in this case is the forging a new signature to indicate non-ownership, based from the original message and original public key corresponding to a unique private/secret key.

(5) With regard to dependent claim 6, Oishi teaches a Group Signature creating apparatus according to claim 5, wherein the signing means comprises hash computing means for computing a hash value for data obtained from a signature/certificate [Col 16, Ln 51] and computational-operation means for performing a computational operation on the hash value computed by the hash computing means [Col 17, Ln 1].

(6) Based from the noted objection/rejection, dependent claim 7 will be interpreted to recite the same limitations as that of its parent claim 5. Hence dependent claim 7 is rejected based on the same rationale as that of its parent claim 5.

With regard to independent and dependent claims 5-7, Oishi does not teach a Ring signature scheme. Since the Ring Signature is a "generalization of the Group Signature" (Naor, 2002), it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the Group Signature cryptographic methods or scheme to that of a Ring signature type as taught by Abe et al (disclosed by the applicant in the Specifications as prior art) because Ring signatures provide the improvement of manager/administrator exclusion.

Non Patent Literature (NPL) Reference:

1. R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret: Theory and Applications of Ring Signatures.

2. M Naor. Deniable Ring Authentication.

3. M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n Signatures from a Variety of Keys.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Jeriko P. San Juan whose telephone number is 571-272-7875. The examiner can normally be reached on M-F 7:30a - 5:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Joseph S Del Sole
JOSEPH S. DEL SOLE
PRIMARY EXAMINER
2/5/07